PART I: CAPITAL ASSET PLAN AND BUSINESS CASE (All Assets)

Agency	U.S. Department of Education				
Bureau	N / A				
Account Title					
Account Identification Code					
Program Activity	Information Dissemination, Information Security				
Name of Project	FSA Single Sign-On – Phase IV				
Unique Project Identifier: (IT only)(See section 53)					
Project Initiation Date	January 31, 2002				
Project Planned Completion Date	September 30, 2003				
This Project is: Initial Concept ____ Planning ____ Full Acquisition __X__ Steady State ____ Mixed Life Cycle ____					
Project / useful segment is funded:		Incrementally	__	Fully	_X__
Was this project approved by OMB for previous Year Budget Cycle?		Yes _X__		No ___	
Did the Executive / Investment Review Committee approve funding for this project this year?		Yes _X__		No ___	
Did the CFO review the cost goal?		Yes _X__		No ___	
Did the Procurement Executive review the acquisition strategy?		Yes _X_		No ___	
Is this investment included in your agency's annual performance plan or multiple agency annual performance plans?		Yes _X__		No ___	
Does the project support homeland security goals and objectives, i.e., 1) improve border and transportation security, 2) combat bio-terrorism, 3) enhance first responder programs; 4) improve information sharing to decrease response times for actions and improve the quality of decision making?		Yes ___		No _X__	
Is this project information technology? (See section 300.4 for definition)		Yes _X__		No ___	
For information technology projects only:					
a. Is this Project a Financial Management System? (see section 53.3 for a definition)		Yes ___		No _X__	
If so, does this project address a FFMIA compliance area?		Yes ___		No ___	
If yes, which compliance area?					
b. Does this project implement electronic transactions or record keeping that is covered by the Government Paperwork Elimination Act (GPEA)?		Yes ___		No _X__	
If so, is it included in your GPEA plan (and does not yet provide an electronic option)?		Yes ___		No ___	
Does the project already provide an electronic option?		Yes ___		No ___	
c. Was a privacy impact assessment performed for this project?		Yes ___		No _X__	
d. Was this project reviewed as part of the FY 2002 Government Information Security Reform Act review process?		Yes ___		No _X__	

d.1 If yes, were any weaknesses found?	Yes ___		No	___
d.2. Have the weaknesses been incorporated into the agency's corrective action plans?	Yes ___		No	___
e. Has this project been identified as a national critical operation or asset by a Project Matrix review or other agency determination?	Yes ___		No	_X__
e.1 If no, is this an agency mission critical or essential service, system, operation, or asset (such as those documented in the agency's COOP Plan), other than those identified above as national critical infrastructures?	Yes ___		No	_X_

SUMMARY OF SPENDING FOR PROJECT STAGES
(In Millions)
(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)

	PY-1 and Earlier	PY 2002	CY 2003	BY 2004	BY+1 2005	BY+2 2006	BY+3 2007	BY+4& Beyond	Total
Planning:									
Budgetary		1.131	0.600						1.731
Outlays		0.605	0.643	0.330	0.122	0.030			1.731
Acquisition :									
Budgetary Resources		2.000	0.705						2.705
Outlays		0.960	1.089	0.454	0.172	0.030			2.705
Total, sum of stages:									
Budgetary Resources		3.131	1.305						4.435
Outlays		1.565	1.732	0.784	0.294	0.060			4.435
Maintenance:									
Budgetary			0.035	1.345	1.152	1.159	1.166	1.213	6.070
Outlays			0.034	0.717	1.052	1.133	1.176	1.960	6.070
Total, All Stages:									
Budgetary		3.131	1.340	1.345	1.152	1.159	1.166	1.213	10.506
Outlays		1.565	1.765	1.501	1.346	1.193	1.176	1.960	10.506

* The BY+4& Beyond costs are estimates only and in no way reflect actual projections for this initiative.

I. A. PROJECT DESCRIPTION

1. Provide a brief description of this project and its status through your capital planning and investment control (CPIC) or capital programming "control" review for the current cycle.

Since the FY 2003 budget submission, Single Sign On has undergone two Control and Select Phase reviews. During FSA's Fall 2001 Select and Control phase reviews, FSA management assessed the initiative's overall health as well as performance against planned cost and schedule. Any areas of improvement associated with this project were identified and corrective actions assigned to the project manager and sponsor. This past

spring Single Sign On was part of the Department's annual combined Select and Control phase. The results of the Control phase review were combined with a thorough assessment of the initiative's value and contribution to the Department. Using these results, the Department's Planning and Investment Review Working Group prioritized Single Sign On against the other IT initiatives in the Department's portfolio. Based on this prioritization, the Department's Investment Review Board made selection and control decisions regarding the composition of the Department's FY 2003 & 2004 IT portfolio. The initiative will undergo the next Control phase review this fall. At that time, the Department will assess performance through fiscal year 2002.

Under the current FSA systems architecture, users in FSA partner organizations (schools, guaranty agencies, lenders, servicers, and state agencies) must use separate logon credentials (user IDs and passwords) to access each FSA system needed to perform their duties. In addition, as new and modernized systems are released, these users may require additional usernames and passwords.

The Single Sign-on initiative reduces the number of usernames and passwords users need to remember to access FSA systems and creates a secure technology infrastructure for logging users in and out of the FSA systems they are authorized to access. The initiative also provides for a common system enrollment process regardless of which FSA system users require access. This result provides FSA with a more secure identification and authentication process while providing FSA's customers with a simpler method to do business with FSA. This enhancement to the FSA systems infrastructure helps FSA accomplish its performance goal of to building and operating systems worthy of trust.

The initiative currently supports the Schools Channel within the Department of Education and FSA. The initiative will expand to support the Financial Partners Channel, as well as additional Schools Channel business applications. In addition, the initiative will support information dissemination and information security.

System users utilize multiple access credentials to logon to FSA systems, which may also have multiple and differing Channel-specific access points. In addition, as new and modernized systems are released, additional access credentials and rights may also be created. This could create increasing opportunities for unauthenticated access to FSA systems, undermining the credibility of FSA, and affecting its ability to help put America through school. The management of multiple user identities is administratively burdensome and costly to FSA and inconvenient to our customers.

- The initiative impact will create a single login and enhanced security for log in to multiple FSA systems.
- Improve customer access to FSA systems – provide a Common user identifier
- Strengthen cyber-security – provision a trusted user identifier

If this effort is not funded, the following are the consequences FSA faces:
- System by system user enrollment will continue.
- System by system user identification will continue.
- System by system user authentication will continue.
- FSA will continue to build new identification and authentication sources for new and reengineered systems.
- Users will have to remember multiple user IDs, passwords and other sign on credentials for multiple systems.
- There will be continued security concerns with respect to the identity of our users and the potential compromise of access credentials.

2. What assumptions are made about this project and why?
It is assumed that the FY2002 implemented Single Sign On solution will be expanded in FY2003 and enable other FSA legacy and modernized systems to reduce their efforts to implement an e-authentication solution.

3. Provide any other supporting information derived from research, interviews, and other documentation.
N / A

I.B. JUSTIFICATION (ALL ASSETS)

1. How does this investment support your agency's mission and strategic goals and objectives?

This initiative covers the continuation of the modernization development and deployment process that began in FY 2001. The initiative supports the development and maintenance of financial integrity with the Department, supports the management of information technology resources, and continued modernization and risk mitigation efforts.

Specifically, the initiative supports Goal 6, Establish Management Excellence, Objectives 6.1, 6.3, and 6.4 of the Department's 2002-2007 Strategic Plan:

- Objective 6.3: Manage information technology resources, using e-gov, to improve service for our customers and partners.
- Objective 6.4: Continue to modernize the Federal Student Aid (FSA) Assistance programs and reduce their high-risk status.

FSA's current legacy system environment has disparate processes and methods to manage user enrollment and sign on. These stove-piped processes create burdens for FSA's customers and increase the overall cost of service delivery. The Single Sign On initiative is projected to will be implementing an electronic enrollment, identification and authentication process for FSA's modernized systems. It is anticipated to provide a single point of access to government services for FSA's customers and partners. It will also provide a standard infrastructure for access management.

Single Sign On is part of the overall FSA Modernization program that seeks to integrate FSA's disparate legacy systems, improve program integrity, reduce costs and improve service to FSA's customers and partners.

2. How does it support the strategic goals from the President's Management Agenda?
Goal 4: Expanded Electronic Government
Objectives:

- Reduce the reporting burden on businesses
- Reduce the expense and difficulty of doing business with the government
- Increase access for persons with disabilities to agency websites and e-Government applications
- Provide high quality customer service regardless of the access channel
- Use the internet to enable citizens to penetrate the Federal bureaucracy to access information and transact business
- Conduct transactions with the public along secure web-enabled systems that use portals to link common applications and protect privacy
- Automate internal processes to reduce costs

This effort enables FSA to participate with the federal e-authentication initiative, as part of the President's e-Gov agenda, by providing a business infrastructure which links to services. E-Authentication is substantiated within FSA vision of "Transitive Trust"; this vision sees users being authenticated by FSA's trusted business partners based on agreed to policies and standards.

Expanded Electronic Government is a primary factor driving SSO's support of the PMA. To enable the e-Government vision, the President's e-Government Taskforce identified initiatives in four categories of electronic service delivery: Service to Individuals; Service to Businesses; Intergovernmental Affairs; and Internal Efficiency and Effectiveness. SSO contributes to the fulfillment of service to individuals that is focused on building easy to find one-stop shops for citizens to create single points of easy entry to access

high quality of governmental services.

3. Are there any alternative sources in the public or private sectors that could perform this function?
Yes; a number of access management solutions are provided by many different vendors. We are developing a solution that best fits business practice needs and is cost effective.

4. If so, explain why your agency did not select one of these alternatives.
Possible solution alternatives did not provide adequate support to the intended strategy.

5. Who are the customers for this project?
This initiative will directly benefit FSA employees, school financial aid administrators, students, and financial partners.

6. Who are the stakeholders of this project?
Other stakeholders include the Department of Education as a whole and its goal to maintain electronic systems with the required level of security capabilities.

7. If this is a multi-agency initiative, identify the agencies and organizations affected by this initiative. N / A

8. How will this investment reduce costs or improve efficiencies?
FSA Single Sign-On will provide the following cost savings and efficiency benefits:
- Improved customer access to FSA systems
- Support the web-based access needs for FSA's Portals and overall eCommerce strategies
- Establish a reusable Single Sign-on service for FSA systems
- Provide potential future economic savings
- User access management
- Reduced customer support for login
- Reduction in the time taken by users in sign-on operations to individual domains, including reducing the possibility of such sign-on operations failing
- Provide development efforts a standard identification and authentication service available for use by all FSA online applications
- A standard Single Sign On authentication service will be developed
- Ease of use of the FSA systems infrastructure should increase over time
- Information accessibility across systems will become transparent to users
- Developers will look to utilize a standard reusable sign-on service

9. List all other assets that interface with this asset.
The SSO capability will be enabled for the following new systems as part of Phase III efforts: eZ-Audit, CRM4FSA, Schools Portal, and Financial Partners portal. It also includes the following critical existing systems – National Student Loan Data System (NSLDS), Central Processing System (CPS), Common Origination & Disbursement (COD), and eCampus Based (eCB) as candidate systems for initial implementation.

Phase IV solution extension to additional systems may include Schools, Students, FP Channels partner-facing systems.

Have these assets been reengineered as part of this project? Yes____, No_X___. Modernized systems have been reengineered as a result of Modernization efforts, but not as part of this project. The SSO capability will provide a reusable service for both legacy and modernized efforts.

I.C. PERFORMANCE GOALS AND MEASURES (ALL ASSETS)

The Single Sign On initiative is currently in the planning phases, thus performance goals and measures have yet to be defined. Performance goals and measures will be targeted during the FY03 efforts.

Fiscal Year	Strategic Goal(s) Supported	Existing Baseline	Planned Performance Improvement Goal	Actual Performance Improvement Results	Planned Performance Metric	Actual Performance Metric Results
2002	N / A	N / A	N / A	N / A	N / A	N / A
2003	Goal 6: Establish Management Excellence; Objectives 6.3, 6.4	TBD	The adoption rate of users having single sign-on loginIDs (number of FSA system users having a "single sign-on" access credential) is targeted for 100% _____ Increase in customer satisfaction, measured by fewer system enrollment processes, fewer system logins and availability of a single, common enrollment service for "single sign-on" enabled systems. _____ Decreased development time will be passed on to other applications since the identification and authentication service, as well as the enrollment service, will be reused (availability of a single, common access control capability for new and reengineered FSA systems). _____ Better access to FSA systems (reduction in the number of credentials a user	N / A	Decreased system access vulnerabilities (measured by the establishment of systems access credentials meeting NIST 800-18 technical control guidelines for identification and authentication) _____ Speed of electronic enrollment for new FSA system users will be improved	N / A

Fiscal Year	Strategic Goal(s) Supported	Existing Baseline	Planned Performance Improvement Goal	Actual Performance Improvement Results	Planned Performance Metric	Actual Performance Metric Results
			requires to access FSA systems). _____ Better security with a standard identification and authentication service for modernized FSA systems will be measured by fewer security breaches.			
2004	Goal 6: Establish Management Excellence; Objectives 6.3, 6.4	TBD	Same as above-Plan to improve targets over time _____ Increase in maintainability due to the reusable and central nature of the identification and authentication and enrollment service (availability of a single, common access control capability for new and reengineered FSA systems). This will be measured by reduced operational costs.	N / A	Same as above-Plan to improve targets over time	N / A
2005	Goal 6: Establish Management Excellence; Objectives 6.3, 6.4	TBD	Same as above-Plan to improve targets over time	N / A	Same as above-Plan to improve targets over time	N / A
2006	Goal 6: Establish Management Excellence; Objectives 6.3, 6.4	TBD	Same as above-Plan to improve targets over time	N / A	Same as above-Plan to improve targets over time	N / A
2007	Goal 6: Establish Management Excellence; Objectives 6.3, 6.4	TBD	Same as above-Plan to improve targets over time	N / A	Same as above-Plan to improve targets over time	N / A

I.D. Program Management [All Assets]

1. Is there a program manager assigned to the project? If so, what is his / her name? Yes X No
   Paul Hill / Neil Sattler
2. Is there a contracting officer assigned to the project? If so, what is his / her name? Yes X No
   Janet Scott
3. Is there an Integrated Project Team? Yes X No

3.A. If so, list the skill set represented.
   Technology, business process, legal
4. Is there a sponsor / owner? Yes X No
   Kay Jacks / Steve Hawald

I.E. Alternatives Analysis [All Assets]

1. Describe the alternative solutions you considered for accomplishing the agency strategic goals that this project was expected to address. Describe the results of the feasibility / performance / benefits analysis. Provide comparisons of the returns (financial and other) for each alternative.

Alternative	Description
Alternative 1 – Selected Alternative	Implementation of an Identification, Authentication, and Unified Enrollment service for *modernized* applications. This provides a standard infrastructure for access management for all modernized systems; single sign-on is an added benefit of this approach. Legacy applications can leverage this infrastructure, as needed.
Alternative 2 –	Implementation of an Identification and Authentication service for existing *legacy* applications. This solution will provide users a single login ID; the technology infrastructure will broker and manage access to legacy systems on the behalf of a user.
Alternative 3 –	Implementation of an Identification, Authentication, and Unified Enrollment service for *legacy* and *modernized* systems. This solution will provide a standard infrastructure for access management for new and legacy systems; single sign-on is a coincident benefit of this alternative. Legacy applications can leverage this infrastructure directly or via a brokering approach, as needed.

Alternative #1 above will establish a business operations and technology infrastructure that provides a:

- Common I&A infrastructure for COD, NSLDS, CPS-FAA, and DLSS
- Unified enrollment capability inter-operate able with the Consistent Answer participation management functionality
- Infrastructure for establishing a common user identifier
- Central user access control repository

SSO will provide future economic savings by establishing a reusable common service for FSA systems, thus reducing operations costs of maintaining separate systems of enrollment, user identification and user authentication.

2. Summarize the results of your life-cycle cost analysis performed for each investment and the underlying assumptions.

all numbers in thousands

Cost Elements	Alternative 1	Alternative 2	Alternative 3

Cost Elements	Alternative 1	Alternative 2	Alternative 3
Contractor Services	$6,221	$6,185.2	$7,760.3
Security Services (PRR, IV&V, C&A)	$450	$400	$400
Hardware (VDC)	$288	N / A	$576
Software	$1,375	N / A	$1,363.2
Training	$66	$66	$66
Total	**$8,400**	**$6,651.2**	**$10,165.6**

Assumptions related to costs above are as follows:

- Life-cycle costs above are estimated over a 5-year duration (FY2002-2007).
- Funding estimates are based on current dollars and do not take into account any inflation or growth estimates.
- Savings are presently undetermined and will likely be assessed during Phase IV initial implementation. It is projected that savings will also be realized through the CRM4FSA project as a result of reduced customer support call volume.
- Hardware and software costs for Alternative 2 are N / A because the hardware and software required for this alternative already exist.
- Acronyms related to security services are as follows:
    - IV&V-Independent Validation and Verification
    - PRR-Production Readiness Review
    - C&A-Certification and Accreditation
- Contractor Services costs include development and operations labor costs
- FTE costs are not factored into the overall costs for the selected alternative; they are not directly attributable to this solution but will be factored into overall FSA budget.

3. Which alternative was chosen and why? Define the Return on Investment (ROI).

This option (Alternative #1 above) will establish a business operations and technology infrastructure that provides a:

- Common I&A infrastructure for COD, NSLDS, CPS-FAA, and DLSS
- Unified enrollment capability inter-operate able with the Consistent Answer participation management functionality
- Infrastructure for establishing a common user identifier
- Central user access control repository

Although Alternative 2 appears less costly, it does not provide the same benefits as Alternative 1. Alternative 2 provides a solution for legacy systems only, and does not include a solution for modernized applications. Additionally, Alternative 2 does not include the unified enrollment capability, nor does it provide a standard infrastructure for access management.

This recommendation is based upon the following criteria:

- Pre-modernization legacy applications will be re-engineered or retired according to the Modernization Blueprint,
- Applications already developed and deployed during FSA Modernization will require a Provisioning mechanism to utilize the standard IAE&P services;
- Each vendors products are rated “Best-of-Breed” by Gartner / Giga
- Each vendor alternative is extendable for eGov initiatives (eAuthentication)
- Each vendor alternative is installed at government & financial organizations
- Each vendor has a history of commitment to the FSA and ED infrastructure
- Enterprise acquisition and ongoing maintenance costs of each finalist are competitive

SSO will provide future economic savings by establishing a reusable common service for FSA systems, thus reducing operations costs of maintaining separate systems of enrollment, user identification and user authentication.

Refer to Section I.F, Risk Inventory and Assessment, for risks related to Alternative 1.
The benefits associated with this alternative do not lend themselves to quantification; thus, the ROI figure cannot be calculated. However, examining the costs, benefits and risks of the alternative altogether identifies this alternative as the most desirable to pursue.

3. A. Are there any quantitative benefits that will be achieved through this investment (e.g., systems savings, cost avoidance, stakeholder benefits, etc)?

Single Sign-On will provide the following benefits:
- Improved customer access to FSA systems
- Supports the web-based access needs for FSA's Portals and overall eCommerce strategies
- Strengthened cyber-security by using a trusted identifier
- Establishes a reusable Single Sign-on service for FSA systems
- Provides potential future economic savings
- User access management
- Reduced customer support for login
- Reduction in the time taken by users in sign-on operations to individual domains, including reducing the possibility of such sign-on operations failing
- Improved security through the reduced need for a user to handle and remember multiple sets of authentication information
- Provides development efforts a standard identification and authentication service available for use by all FSA online applications
- Improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration including the ability to inhibit or remove an individual users' access to system resources in a coordinated and consistent manner

Short-term benefits include the following:
- A baseline Single Sign-On for an estimated 20,000 FSA system users
- Stronger security through consistent user identification and authentication

The long-term implications may include the following:
- Customer utility will increase
- User support services will improve
- A standard Single Sign On authentication service will be developed
- Ease of use of the FSA systems infrastructure should increase over time
- Information accessibility across systems will become transparent to users
- Developers will look to utilize a standard reusable sign-on service

The following tables provide further benefits related to customer and employee satisfaction:

Quantified/Qualitative Benefit	How will benefit be measured/realized?	When will benefit be realized?
Financial Aid Professionals will save time accessing FSA systems - NSLDS, DLSS, COD and Schools Portal.	Final Acceptance interviews with customers (e.g., FAP ability to perform / complete responsibilities improved has improved).	Immediately after upon conclusion of implementation.

Quantified/Qualitative Benefit	How will benefit be measured/realized?	When will benefit be realized?
Financial Aid Professionals will have a reduced number of username and passwords needed to access NSLDS, DLSS, COD, and Schools Portal.	One username and password for accessing multiple systems.	Immediately upon conclusion of implementation.
Customers will have a greater trust in systems with a stronger security framework.	Final Acceptance interviews with customers (e.g., perceived level of trust in SFA systems is higher).	Immediately upon conclusion of implementation.
Customers may have authorized access to more FSA systems that are integrated into the Authentication gateway in the future.	Number of systems integrated into the Authentication gateway after completion.	A long-term benefit. Not a measurable benefit of the initial baseline SSO project.
Students will have an easier time accessing information from Financial Aid Professionals.	Final Acceptance interviews with customers (e.g., Financial Aid Professionals are able to satisfy a greater number of service requests the first time).	An indirect benefit from Financial Aid Professional increased productivity.
Assumptions		
The Single Sign-On baseline implementation will be successful and reusable for future systems. Potential customer satisfaction measurements to quantify success of SSO project might include: • Transactions performed / completed before / after SSO. • Transaction errors before / after • Calls to help desk to change / renew password / PIN In order to measure customer satisfaction improvement, baseline (current) data and process improvement identifiers and data collection mechanisms are required. Otherwise the customer satisfaction improvements are not auditable.		

Quantified/Qualitative Benefit	How will benefit be measured/realized?	When will benefit be realized?
Employees will have happier customers.	Final Acceptance interviews with customers (e.g., Financial Aid Professionals are able to satisfy a greater number of service requests the first time).	Immediately upon conclusion of implementation.
Employees will have a standard authentication framework to build from.	How many systems will be integrated with the Authentication Gateway.	Long-term benefit. Not a measurable benefit of the initial baseline SSO project.
FSA systems will present a unified means of accessing information, thereby increasing their reputation of a reputable financial technology leader.	How many systems will be integrated with the Authentication Gateway.	Long-term benefit. Not a measurable benefit of the initial baseline SSO project.
Assumptions		
The Single Sign-On baseline implementation will be successful and reusable for future systems.		

3. B. FOR ALTERNATIVE SELECTED, PROVIDE FINANCIAL SUMMARY, INCLUDING NET PRESENT VALUE BY YEAR AND PAYBACK PERIOD CALCULATIONS:

The financial summary below indicates the net present value by year and in total for this initiative.

NPV	2002	2003	2004	2005	2006	2007	Total
SSO	-3,130.7	-1,282.0	-1,232.0	-1,009.4	-971.8	-935.6	-8,561.4

The primary benefits of the initiative, as outlined in 3.A above, are of a qualitative nature and cannot be included in the payback period equation. As a result, the quantified savings associated with this initiative are not greater than the investment to undertake it, making it impossible to calculate the payback period financial measure. However, examining the costs, benefits and risks of the alternative altogether as presented above, identifies this alternative as the most desirable to pursue.

4. What is the date of your cost benefit analysis? 05/3/2002 – Costs and benefits were documented in the FY03-04 Select Phase Single Sign On Business Case.

I. F. Risk Inventory and Assessment (All Assets)

In this section, describe the results of your risk assessment for this project and discuss your plans to eliminate, mitigate, or manage identified risks. Risk assessments should be performed at the initial concept stage and then monitored and controlled throughout the life-cycle of the project, and should include risk information from all stakeholders. Risk assessments for all projects must include schedule, costs (both initial and life cycle), technical obsolescence, feasibility, reliability of systems, dependencies and interoperability between this project and others, surety (asset protection) considerations, risk of creating a monopoly for future procurements, capability of agency to manage the project, and overall risk of project failure.

In addition, for IT projects risk must be discussed in the following categories 1) Organizational and Change Management, 2) Business, 3) Data/Info, 4) Technology, 5) Strategic, 6) Security, 7) Privacy, and 8) Project Resources. (Agencies may include others for IT, and may define the core set for other assets). For security risks, identify under the description column the level of risk as high, medium, or basic. What aspect of security determines the level of risk, i.e., the need for confidentiality of information, availability of information or the system, reliability of the information or system?

Date Identified	Area of Risk	Description	Probability of Occurrence	Strategy for Mitigation	Current Status as of the date of this exhibit
5/3/2002	Strategic	Single Sign-On is a component of the FSA Modernization Blueprint to provide increased customer service and a single identification and authentication standard for FSA	Low	Input from the Department, FSA, customers, industry groups and other Federal e-Gov initiatives will be included to ensure compatibility of the FSA single sign-on solution.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.

Date Identified	Area of Risk	Description	Probability of Occurrence	Strategy for Mitigation	Current Status as of the date of this exhibit
		applications. An appropriate standard for identification and authentication needs to be developed.			
5/3/2002	Organizational /Change Management	This enterprise service function will need to be managed centrally by FSA.	Low	Appropriate recommendations will be made at the conclusion of Phase III.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.
	Project Resources (Financial, Personnel, etc.)	Security, Identification and Authentication and single sign-on enabled system-specific authentication resources will be required to implement a successful solution.	Low	The project team will be comprised of resources knowledgeable on security, identification and authentication and FSA systems.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.
	Project Management	The project will need coordination across all the life cycle stages as well as resources, technology, and applicable standards.	Low	An IPT (Integrated Product team) approach will be utilized to ensure timely participation and contribution.	This risk has not occurred. This risk has been successfully mitigated. This risk is still applicable.
	Business	The FSA customers will need to adopt this single sign-on solution for single login and access to FSA systems.	Low	Phase III and Phase IV activities will include community outreach tasks to ensure comprehensive understanding of new service.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.

Date Identified	Area of Risk	Description	Probability of Occurrence	Strategy for Mitigation	Current Status as of the date of this exhibit
	Data / Information	Login data will be maintained within the appropriate single sign-on data store.	Low	The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations.	This risk has occurred. We are in the process of mitigating this risk. This risk is still applicable.
	Application	Connectors from single sign-on to FSA systems will be required.	Low	Industry and Federal standard techniques will be utilized to implement COTS / GOTS connectors from the single sign-on facility to enabled systems.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.
	Technology / Infrastructure	The single sign-on technology is maturing, the federal standards for cross-organization identification and authentication are evolving, and appropriate infrastructure will be required.	Low	Phase III will implement technology compatible with the evolving e-Gov e-Authentication standards, PAMs (Pluggable Authentication Modules) to support additional identification and authentication sources and the infrastructure will be scaled to handle the required capacity.	This risk has occurred. We are in the process of mitigating this risk. This risk is still applicable.
5/3/5/3	Security	Login data will be maintained within the single sign-on data store to support single login.	Low	The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations.	This risk has not occurred. We are in the process of mitigating this risk. This risk is still applicable.

1. What is the date of your risk management plan? 5/3/2002 – Risks and associated mitigation plans were documented in the FY03-04 Select Phase Single Sign On Business Case.

I.G. Acquisition Strategy

1. Will you use a single contract or several contracts to accomplish this project?
Single Contract

1.A. If multiple contracts are planned, explain how they are related to each other, and how each supports the project performance goals. N/A

2. What type(s) of contract(s) will you use (e.g. cost reimbursement, fixed-price, etc.)?

This initiative will be contracted as Firm Fixed Price contract with the FSA Modernization Partner. The contract type is a Blanket Purchase Agreement (BPA) under GSA Schedule 70 Contract (GS-35F-4692G) implemented using Task Orders (FP, FP Share in Savings IF, and T&M)

2.A. For cost reimbursement contracts, define risk not sufficiently covered by the risk mitigation plan to require this type of contract. N/A

3. Will you use financial incentives to motivate contractor performance (e.g. incentive fee, award fee, etc.)?
No

4. Will you use competition to select suppliers?
SSO Phase II included an Alternatives Evaluation; a vendor was recommended and selected as a result of the evaluation.

5. Will you use commercially available or COTS products, or custom-designed products?
Yes. 51-75% of the project will be COTS.

6. What is the date of your acquisition plan?
5/3/2002 - An acquisition overview was documented in the FY03-04 Select Phase Single Sign On Business Case.

7. How will you ensure Section 508 compliance?
Compliance with Section 508 will be ensured contractually through test plans. Additionally, support from the Department's Assistive Technology team will be required to ensure Section 508 compliance once hardware and software have been identified.

The Department of Education does follow the following multi-step process to ensure Section 508 compliance for both COTS and customized software development products:

- Include language in the contract that states that all EIT equipment will meet applicable 508 standards.
- Ask respondents to advise the government how they will meet the accessibility requirements.
- Require the contractor deliver all documentation and manuals in an electronic format compatible with the Assistive Technology currently in use at the Department.
- Require design reviews and development testing of the software by the Education Assistive Technology team for accessibility.

I.H. Project and Funding Plan

The information required by this section will be provided by your earned value management system (EVMS)

and the EVMS software program you use that meets the ANSI/EIA Standard 748 (see section 300.4 (earned value management)). Information on earned value management systems is available at http://www.acq.osd.mil/pw.

I.H.1. Description of performance-based management system (PBMS):

Name the software program that meets ANSI/EIA Standard 748 that you will use, or are using, to monitor and manage contract and project performance. If the project is operational (steady state), define the operational analysis system that will be used. If this is a mixed life-cycle project with both operational and development/modernization/ enhancement (DME) system improvement aspects, EVMS must be used on the system improvement aspects of the contract and operational analysis on the operations aspects. Using information consistent with the work breakdown structure (WBS), provide the information requested in all parts of this section.

The Department uses a work breakdown structure and associated cost estimates to create a cost and schedule of milestones for a project. We measure performance against the planned cost and schedule of milestones. Currently, the Department uses an Excel workbook to collect, maintain, and calculate earned value information. We intend to use the recently revised Earned Value Management System (EVMS) that is integrated with the Information Technology Investment Portfolio System (I-TIPS) as our performance based management system (PBMS). As part of the Select and Control phase of the Department's IT investment management (ITIM) process, project managers provide planned cost and schedule information for their development milestones. This information provides the baseline against which actual cost and schedule performance is collected and measured. With the baseline and actual data provided by the project managers, the Department conducts an earned value analysis of the projects. The result of this analysis feeds directly into the assessment of the project's health, which impacts the overall select and control decisions made about the investment. If an initiative's variance approaches -10%, the Department directs corrective actions that are monitored until the variance is eliminated or there is strong evidence that no further increases in the negative variance will occur.

I.H.2. Original baseline (OMB-approved at project outset):

What are the cost and schedule goals for this phase or segment/module of the project (e.g., what are the major project milestones or events; when will each occur; and what is the estimated cost to accomplish each one)? Also identify the funding agency for each milestone or event if this is a multi-agency project. If this is a multi-agency project or one of the President's E-Gov initiatives, use the detailed project plan with milestones on the critical path, to identify agency funding for each module or milestone. (This baseline must be included in all subsequent reports, even when there are OMB-approved baseline changes shown in I.H.3).

Cost and Schedule Goals: Original Baseline for a Phase/Segment/Module of Project					
	Schedule				
Description of Milestone	Start Date	End Date	Duration (in days)	Planned Cost	Funding Agency
1. Ph 1 - Requirements Definition	1/7/02	3/15/02	67	250,000	Dpt. of Education-Federal Student Aid (FSA)
2. Ph 2 - General Design and Recommendation	3/18/02	6/19/02	93	250,000	Dpt. of Education-Federal Student Aid (FSA)
3. Ph 3 - Development	06/20/02	09/30/02	102	1,594,300	Dpt. of Education-

					Federal Student Aid (FSA)
4. Ph 3 – Deployment for Initial Systems	10/01/02	12/31/02	91	905,800	Dpt. of Education-Federal Student Aid (FSA)
5. Ph 4 – Requirements for Unified Enrollment	1/1/03	5/31/03	150	500,000	Dpt. of Education-Federal Student Aid (FSA)
6. Ph 4 – Extended Deployment	1/1/03	9/30/03	272	700,000	Dpt. of Education-Federal Student Aid (FSA)
Completion date: 09/30/03				Total cost estimate at completion: 4,200,000	
FY2004 Maintenance				$1,200,000	
FY2005 Maintenance				$1,000,000	
FY2006 Maintenance				$1,000,000	
FY2007 Maintenance				$1,000,000	

I.H.3. Proposed baseline/current baseline (applicable *only* if OMB-approved the changes):

Identify in this section a proposed change to the original or current baseline or an OMB-approved baseline change. What are the new cost and schedule goals for the project (e.g., what are the major project milestones or events; when will each occur; and what is the estimated cost to accomplish each one)? Also identify the funding agency for each milestone or event if this is a multi-agency project. If this is a new project in the FY 2004 budget year, this section will be blank for your initial submission.

Cost and Schedule Goals: Proposed_____ or Current (OMB-Approved)_____ Baseline for a Phase/Segment/Module of Project					
	Schedule				
Description of Milestone	Start Date	End Date	Duration (in days)	Planned Cost	Funding Agency
1.					
2.					
3.					
Completion date:				**Total cost estimate at completion:**	

I.H.4 ACTUAL PERFORMANCE AND VARIANCE FROM OMB-APPROVED BASELINE (ORIGINAL OR CURRENT):

A. Show for each major project the milestones or events you planned (scheduled) to accomplish and the cost and what work was actually done and the cost. If this is a new project in the FY 2004 budget year, this section will be blank for your initial submission. OMB may ask for the latest information during the budget review process.

Comparison of OMB-Approved Baseline and Actual Outcome for Phase / Segment / Module of a Project									
Description of Milestone	OMB-Approved Baseline					Actual Outcome			
	Schedule					Schedule			
	Start Date	End Date	Duration (in days)	Planned Cost	Funding Agency	Start Date	End Date	Percent Complete	Actual Cost
1.									
2.									
3.									
Completion date: OMB-approved baseline:						**Estimated completion date:**			
Total cost: OMB-approved baseline:						**Estimate at completion:**			

B. Provide the following project summary information from your EVMS software: As of : (date)

B.1. Show the budgeted (planned) cost of work scheduled (BCWS): $ _____

B.2. Show budgeted (planned) cost of work performed (BCWP): $ _____

B.3. Show the actual cost of work performed (ACWP): $ _____

B.4. PROVIDE A COST CURVE GRAPH PLOTTING BCWS, BCWP AND ACWP ON A MONTHLY BASIS FROM INCEPTION OF THIS PHASE OR SEGMENT / MODULE THROUGH THE LATEST REPORT. IN ADDITION, PLOT THE ACWP CURVE TO THE ESTIMATED COST AT COMPLETION (EAC) VALUE, AND PROVIDE THE FOLLOWING EVMS VARIANCE ANALYSIS.

PROJECT SUMMARY (CUMULATIVE)	
	Value
Cost Variance = (BCWP-ACWP) =	
Cost Variance % = (CV/BCWP) x 100% =	
Cost Performance Index (CPI) = (BCWP/ACWP) =	
Schedule Variance = (BCWP-BCWS) =	
Schedule Variance % = (SV/BCWS) x 100% =	
Schedule Performance Index (SPI) = (BCWP/BCWS) =	
Two independent Estimates at Completion (EAC) = (ACWPcum + Performance Factor (PF) X(BAC B BCWPcum) where PF_1 = 1/CPI, and PF_2 = 1/CPI x SPI =	
Variance at Completion (VAC) = (BAC B EAC) for both EACs above =	
Variance at Completion % = (VAC/BAC) x 100% for both EACs above =	
Expected Funds to Completion (ETC) =	
Expected Completion Date =	

Definitions for Earned Value Management System:

ACWP – Actual Cost for Work Performed – What you paid.
BAC – Budget At Completion – The baseline (planned) budget for the project.
BCWP – Budgeted Cost for Work Performed – The earned value.
BCWS – Budgeted Cost for Work Scheduled – The planned costs.
CPI – Cost Performance Index – The ratio of the budgeted to actual cost of work performed.
CV – Cost Variance – The difference between planned and actual cost of work performed.
EAC – Estimate At Completion – The latest estimated cost at completion.
ETC – Estimate to Completion – Funds needed to complete the project.
PF – Performance Factor – The cost to earn a dollar of value, or ACWP/BCWP, or 1/CPI.
SPI – Schedule Performance Index – The percent of the project that has been completed.
SV – Schedule Variance – The variance between the actual and planned schedules.
VAC – Variance at Completion – The variance between the baseline and actual budget at completion.

C. If cost and/or schedule variance are a negative 10 percent or more, explain the reason(s) for the variance(s):

D. Provide performance variance. Explain whether, based on work accomplished to date, you still expect to achieve your performance goals. If not, explain the reasons for the variance.

E. Discuss the contractor, government, and at least the two EAC index formulas in I.H.4.B, current estimates at completion. Explain the differences and the IPTs selected EAC for budgeting purposes.

Discuss the corrective actions that will be taken to correct the variances, the risk associated with the actions, and how close the planned actions will bring the project to the original baseline. Define proposed baseline changes, if necessary.

F. Has the Agency Head concurred in the need to continue the program at the new baseline?
Yes____ No____

Part II: Additional Business Case Criteria for Information Technology

II. A. Enterprise Architecture

II.A.1 Business

A. Is this project identified in your agency's enterprise architecture? If not, why?
Yes. It is identified in the FSA Modernization Blueprint, which is part of the agency's enterprise architecture.

B. Explain how this project conforms to your departmental (entire agency) enterprise architecture.
The construction of the target business enterprise architecture is based on three basic functional areas: administrative; K-12; and post-secondary education. In accordance with the One-ED process above, the business processes SSO supports will be included in the business process reviews. The One-ED process will begin with identification of the business functions, then conducting business case analyses, followed by re-engineering or competitive sourcing decisions. Three outcomes are possible: the status quo in which we continue work as is; competition with best value alternatives decisions; or business process re-engineering. Under the competition alternative, two options are possible: employee best value wherein the business process will be re-engineered in-house; or the industry best value wherein the business process will be transitioned and re-engineered outside the agency. The agency One-ED initiative lists and defines all agency activities and groups them by One-ED phase. The One-ED is scheduled by phases. All business process re-engineering, or competitive sourcing decisions will be made subsequent to the phased One-ED business case analyses. The agency baseline enterprise architecture will be a basic part of the analytical process.

C. Identify the Lines of Business and Sub-Functions within the Federal Enterprise Architecture Business Reference Model that will be supported by this initiative.
Federal Financial Assistance-Grants Assistance, Loans Assistance

D. Briefly describe how this initiative supports the identified Lines of Business and Sub-Functions of the Federal Business Architecture.
The initiative supports modernization initiatives within the FSA enterprise for identity management of users across the channels. All future modernization initiatives will utilize the common identification and authentication service to provide access to FSA systems. Additionally, the modernized initiatives will utilize the common system enrollment service for the generation of identification and authentication. Specifically, the initiative will integrate with the Title IV participation management function to provide system enrollment services within the Schools and Financial Partners channels. The initiative will benefit the Students channel by allowing students to login once for transactions associated with multiple back-end systems. The initiative will support information dissemination and information security.

E. Was this project approved through the EA Review committee at your agency?
No projects have gone through the EA Review committee process to date. The Deputy Chief Information Officer for Information Management chartered the recently established Enterprise Architecture Working Group (EAWG), a sub-group of the Information Management Working Group. Its membership represents major business units in the agency. In cooperation with the agency's procurement executive, the EAWG will review projects before they are entered into the acquisition process. The EAWG's role is specified in the Enterprise Architecture Configuration Management process, as are related reviews by the Technology Review Board and the Configuration Control Review Board. The former reviews projects in development and the latter reviews them after implementation. The EAWG reviews projects before acquisition and monitors reviews by the other two review bodies. Until the target enterprise architecture is complete, with its transition plan, the EAWG will be limited to reviewing projects in terms of their capabilities and services. The EAWG is developing and will keep current advanced capabilities that have been identified as part of the target technical operating environment that will be used for project reviews. This year, as in years past, each business case was reviewed for consistency in the Product Support Plan, which is based on our architectural standards. Each Principal Office is encouraged to have internal review processes in place for the Capital

Planning and Investment Management process, and those processes may include formal architectural reviews.

Within FSA, projects have gone through an FSA Architecture Review Committee process. The FSA Deputy Chief Information Officer for Enterprise IT Management signs off on the business case that the enterprise architecture review has been completed. The review is completed in terms of business alignment as well as compliance with established standards and policies.

Additionally, this project was reviewed by the FSA Investment Review Board to ensure business and technical architecture aligns with the agency's architecture.

F. What are the major process simplification / reengineering / design projects that are required as part of this initiative?
Reengineering and design efforts will focus on the process of providing access to services that customers are entitled to access without having to identify and authenticate him / herself multiple times. A new process to enroll new users to systems that are Single Sign-On enabled will also be determined. This process will provision a user's single sign-on access credentials, back-end system credentials, and obtain user profile data.

G. What are the major organization restructuring, training, and change management projects that are required?
The overall technical architecture and security framework for FSA is an integral part of this single sign-on solution. Internal and external users of FSA business systems will be trained and provided the opportunity to enable themselves to access with a single login those FSA systems in which they are enrolled.

H. What are the Agency lines of business involved in this project?
Information Dissemination and Information Security

I. What are the implications for the agency business architecture?
FSA projects are compliant with the Modernization Blueprint, which is the essence of the target architecture for post-secondary education.

II.A.2 Data

A. What types of data will be used in this project?
Not Applicable; Data is not involved in this project.

B. Does the data needed for this project already exist at the Federal, State, or Local level? If so, what are your plans to gain access to that data?
Not Applicable; Data is not involved in this project.

C. Are there legal reasons why this data cannot be transferred? If so, what are they and did you address them in the barriers and risk sections above?
Not Applicable; Data is not involved in this project.

D. If this initiative processes spatial data, identify planned investments for spatial data and demonstrate how the agency ensures compliance with the Federal Geographic Data Committee standards required by OMB Circular A–16.
Not Applicable; Data is not involved in this project.

II.A.3 Application and Technology

A. Discuss this initiative / project in relationship to the application and technology layers of the EA. Include a discussion of hardware, applications, infrastructure, etc.

Vendor selection and product review is currently in process.

B. Are all of the hardware, applications, and infrastructure requirements for this project included in the EA Technical Reference Model? If not, please explain.
Vendor selection and product review is currently in process.

II. B. SECURITY AND PRIVACY

NOTE: Each category below must be addressed at the project (system / application) level, not at a program or agency level. Referring to security plans or other documents is not an acceptable response.

II.B.1. How is security provided and funded for this project (e.g., by program office or by the CIO through the general support system / network)?
Security is provided and funded for each of the Department's IT initiatives through the responsible program office. In this case, security is provided and funded for SSO through FSA.

A. What is the total dollar amount allocated to security for this project in FY 2004? $50,000

II.B.2 Does the project (system / application) meet the following security requirements of the Government Information Security Reform Act, OMB policy, and NIST guidance?

A. Does the project (system / application) have an up-to-date security plan that meets the requirements of OMB policy and NIST guidance? What is the date of the plan?
Security plans of participating systems will need to reflect new authentication capability resulting from this initiative. This is not an existing FSA system, and is not required to meet GISRA's reporting requirements.

B. Has the project undergone an approved certification and accreditation process? Specify the C&A methodology used (e.g., NIST guidance) and the date of the last review. No, this project is still in the planning phases; the certification and accreditation process will be completed prior to system implementation.

C. Have the management, operational, and technical security controls been tested for effectiveness? When were most recent tests performed?
No, this project is still in the planning phases.

D. Have all system users been appropriately trained in the past year, including rules of behavior and consequences for violating the rules?
No, this project is still in the planning phases.

E. How has incident handling capability been incorporated into the system, including intrusion detection monitoring and audit log reviews? Are incidents reported to GSA's FedCIRC?
An incident handling capability has not yet been incorporated into this system. However, the Department of Education is currently in the process of establishing a Department-wide intrusion detection program, which will address intrusion detection monitoring, audit log reviews, and incident reporting to GSA as dictated by OMB Circular A-130. The Department-wide program will not meet this requirement, but will serve as a basis for individual systems to implement incident handling capabilities.

F. Is the system operated by contractors either on-site or at a contractor facility? If yes, does any such contract include specific security requirements required by law and policy? How are contractor security procedures monitored, verified, and validated by the agency?"
No, this project is still in the planning phases.

II.B.3 How does the agency ensure the effective use of security controls and authentication tools to protect privacy for those systems that promote or permit public access?
As soon as an initiative is undertaken, a General Support System and Major Application Inventory Submission Form is completed to register the system. In doing so, the system is evaluated for maintenance of personal information. If it is determined that the system will store or process personal information, a notice of a Privacy Act System of Records is published in the Federal Register for public comment. The system notice describes the measures that will be taken to prevent unauthorized disclosure of records at a level of security that indicates the sufficiency of the safeguards without providing such detail that it increases the risk of unauthorized access to the records. As a part of the Department's certification and accreditation (C&A) process, a system risk assessment is performed which further evaluates the type of data that will be stored / processed by the system and the security controls that will be applied. Development of measures and controls, or remediation of deficiencies, to protect privacy information is established in the system security plan in accordance with the Department's policy and guidance. Through the Department's C&A process and associated documents, we ensure effective use of security controls and authentication tools to protect privacy information.

II.B.4 How does the agency ensure that the handling of personal information is consistent with relevant government-wide and agency policies.
As soon as an initiative is undertaken, a General Support System and Major Application Inventory Submission Form is completed to register the system. In doing so, the system is evaluated for maintenance of personal information. If it is determined that the system will store or process personal information, a notice of a Privacy Act System of Records is published in the Federal Register for public comment. The system notice describes the measures that will be taken to prevent unauthorized disclosure of records at a level of security that indicates the sufficiency of the safeguards without providing such detail that it increases the risk of unauthorized access to the records. As a part of the Department's certification and accreditation (C&A) process, a system risk assessment is performed which further evaluates the type of data that will be stored / processed by the system and the security controls that will be applied. Development of measures and controls, or remediation of deficiencies, to protect privacy information is established in the system security plan in accordance with the Department's policy and guidance. Through the Department's C&A process and associated documents, we ensure effective use of security controls and authentication tools to protect privacy information.

II.B.5 If a Privacy Impact Assessment was conducted, please provide a copy to OMB. N / A

II. C. GOVERNMENT PAPERWORK ELIMINATION ACT (GPEA)

II.C.1 If this project supports electronic transactions or record-keeping that is covered by GPEA, briefly describe the transaction or record-keeping functions and how this investment relates to your agency's GPEA plan.
N / A

II.C.2 What is the date of your GPEA plan?
N / A

II.C.3 Identify any OMB Paperwork Reduction Act (PRA) control numbers from information collections that are tied to this investment.
N / A